

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-344441

(43)Date of publication of application : 29.11.2002

(51)Int.Cl.

H04L 9/14
G06F 12/14
G09C 1/00

(21)Application number : 2001-142204

(71)Applicant : RICOH CO LTD

(22)Date of filing : 11.05.2001

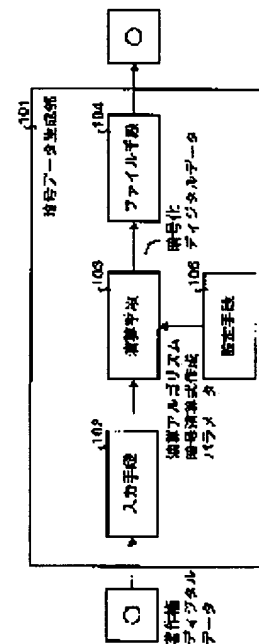
(72)Inventor : NASU MASAMI

(54) DIGITAL DATA ENCRYPTION SYSTEM, DIGITAL DATA REPRODUCING DEVICE, DIGITAL DATA ENCIPHERING METHOD, DIGITAL DATA REPRODUCING METHOD AND PROGRAM FOR MAKING COMPUTER EXECUTE THE METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To protect the copyright of digital data, without imposing constraints on the use condition of a personal computer or the like, or affecting the costs of a digital data reproducing device.

SOLUTION: An input means 102 reads copyright digital data stored in a recording medium, such as CD-ROM, and an arithmetic means 103 selects a plurality of cryptographic algorithms set by a setting means 105 from a cryptographic arithmetic formula preparing parameter, and enciphers the copyright digital data according to the cryptographic arithmetic formula which is decided based on the selection. A file means 104 creates not only the enciphered digital data but also an index value and the cryptographic arithmetic formula preparing parameter in the same file, and outputs it to a flash memory. A reproduction device obtains the cryptographic arithmetic formula from the index value and the cryptographic arithmetic formula preparing parameter in the same file as that of the enciphered digital data, and reproduces digital data by carrying out corresponding decoding processing.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-344441
(P2002-344441A)

(43) 公開日 平成14年11月29日 (2002. 11. 29)

(51) Int.Cl. ⁷	識別記号	F I	テマコード [*] (参考)
H 0 4 L 9/14		G 0 6 F 12/14	3 2 0 B 5 B 0 1 7
G 0 6 F 12/14	3 2 0		3 2 0 E 5 J 1 0 4
		G 0 9 C 1/00	6 4 0 D
G 0 9 C 1/00	6 4 0	H 0 4 L 9/00	6 4 1

審査請求 未請求 請求項の数14 O L (全 11 頁)

(21) 出願番号 特願2001-142204(P2001-142204)

(22) 出願日 平成13年 5 月11日 (2001. 5. 11)

(71) 出願人 000006747

株式会社リコー

東京都大田区中馬込 1 丁目 3 番 6 号

(72) 発明者 奈須 政巳

東京都大田区中馬込 1 丁目 3 番 6 号 株式
会社リコー内

(74) 代理人 100104190

弁理士 酒井 昭徳

Fターム (参考) 5B017 AA06 BA07 CA15

5J104 AA08 AA16 AA34 EA02 EA04

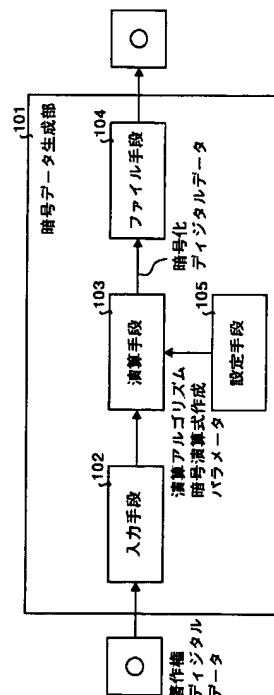
EA23 PA14

(54) 【発明の名称】 デジタルデータ暗号システム、デジタルデータ再生装置、デジタルデータ暗号方法、デジタルデータ再生方法およびそれらの方法をコンピュータに実行させるプログラム

(57) 【要約】

【課題】 パーソナルコンピュータなどの使用条件に制約をおよぼすことなく、またデジタルデータ再生装置のコストに影響を与えずにデジタルデータの著作権を保護すること。

【解決手段】 入力手段 1 0 2 は C D - R O M などの記録媒体に格納された著作権デジタルデータを読み取り、演算手段 1 0 3 は設定手段 1 0 5 に設定された複数の暗号アルゴリズムを暗号演算式作成パラメータから選択し、この選択に基づき決定される暗号演算式にしたがって著作権デジタルデータを暗号処理し、ファイル手段 1 0 4 は暗号化デジタルデータとともに、インデックス値と暗号演算式作成パラメータを同一のファイルに作成しフラッシュメモリなどに出力する。再生装置は暗号化デジタルデータと同一ファイルのインデックス値と暗号演算式作成パラメータから暗号演算式を得て対応する復号処理をして再生する。



【特許請求の範囲】

【請求項1】 入力されたデジタルデータを所定の暗号アルゴリズムおよび暗号演算式作成パラメータに基づき決定される暗号演算式にしたがって、暗号処理をおこなう演算手段と、

前記暗号化されたデジタルデータとともに、暗号処理に用いた暗号アルゴリズムを一意に決定可能なインデックス値と暗号演算式作成パラメータを、同一のファイルに作成出力するファイル手段と、
を備えたことを特徴とするデジタルデータ暗号システム。

【請求項2】 実際の暗号化に使用する暗号アルゴリズムがあらかじめ複数設定登録された設定手段を備え、前記暗号処理時に所定の暗号アルゴリズムが選択可能なことを特徴とする請求項1に記載のデジタルデータ暗号システム。

【請求項3】 前記演算手段は、前記暗号処理時に、あらかじめ用意された複数の暗号アルゴリズムおよび暗号演算式作成パラメータの中から実際の暗号化に使用する暗号アルゴリズムおよび暗号演算式作成パラメータを選択し、該選択した暗号アルゴリズムおよび暗号演算式作成パラメータを用いて、暗号処理をおこなうことを特徴とする請求項1に記載のデジタルデータ暗号システム。

【請求項4】 前記演算手段は、前記暗号アルゴリズムに基づきデジタルデータの任意の場所に特定のデータ改ざん検出コードを埋め込み暗号処理を実行することにより、デジタルデータの不正改ざんを検出可能なことを特徴とする請求項1～3のいずれか一つに記載のデジタルデータ暗号システム。

【請求項5】 前記ファイル手段は、前記暗号化デジタルデータと同一ファイルに格納する暗号アルゴリズムのインデックス値および暗号演算式作成パラメータの記載箇所を容易に特定できない状態となるようデータ変更を施すことを特徴とする請求項1～4のいずれか一つに記載のデジタルデータ暗号システム。

【請求項6】 請求項1～5のいずれかのデジタルデータ暗号システムにより生成された暗号化デジタルデータから著作物デジタルデータを復号、再生するデジタルデータ再生装置であって、

前記暗号化されたデジタルデータを取り込む読み取り手段と、

前記暗号化されたデジタルデータと同一ファイル内に記載された暗号アルゴリズムのインデックス値、および暗号演算式作成パラメータに基づく暗号演算式を決定し、その演算式にしたがって前記暗号化されたデジタルデータの復号処理をおこなう演算手段と、

前記復号化により再現された元のデジタルデータを再生出力する再生手段と、

を備えたことを特徴とするデジタルデータ再生装置。

【請求項7】 前記演算手段は、前記暗号化デジタルデータの任意の場所に埋め込まれた特定のデータ改ざん検出コードの検出の有無に基づき、デジタルデータの改ざんの有無を判断し、不正改ざんと判断した場合には、再生しないことを特徴とする請求項6に記載のデジタルデータ再生装置。

【請求項8】 入力されたデジタルデータを所定の暗号アルゴリズムおよび暗号演算式作成パラメータに基づき決定される暗号演算式にしたがって、暗号処理をおこなう演算工程と、

前記暗号化されたデジタルデータとともに、暗号処理に用いた暗号アルゴリズムを一意に決定可能なインデックス値と暗号演算式作成パラメータを、同一のファイルに作成出力するファイル工程と、

を含んだことを特徴とするデジタルデータ暗号方法。

【請求項9】 前記演算工程は、あらかじめ用意された複数の暗号アルゴリズムおよび暗号演算式作成パラメータの中から実際の暗号化に使用する暗号アルゴリズムおよび暗号演算式作成パラメータを選択し、該選択した暗号アルゴリズムおよび暗号演算式作成パラメータを用いて、暗号処理をおこなうことを特徴とする請求項8に記載のデジタルデータ暗号方法。

【請求項10】 前記演算工程は、前記暗号アルゴリズムに基づきデジタルデータの任意の場所に特定のデータ改ざん検出コードを埋め込み暗号処理を実行することにより、デジタルデータの不正改ざんを検出可能なことを特徴とする請求項8、9のいずれか一つに記載のデジタルデータ暗号方法。

【請求項11】 前記演算工程は、前記暗号化デジタルデータと同一ファイルに格納する暗号アルゴリズムのインデックス値および暗号演算式作成パラメータの記載箇所を容易に特定できない状態となるようデータ変更を施すことを特徴とする請求項8～10のいずれか一つに記載のデジタルデータ暗号方法。

【請求項12】 請求項8～10のいずれかのデジタルデータ暗号方法により生成された暗号化デジタルデータから著作物デジタルデータを復号、再生するデジタルデータ再生方法であって、

前記暗号化されたデジタルデータを取り込む読み取り工程と、

前記暗号化されたデジタルデータと同一ファイル内に記載された暗号アルゴリズムのインデックス値、および暗号演算式作成パラメータに基づく暗号演算式を決定し、その演算式にしたがって前記暗号化されたデジタルデータの復号処理をおこなう演算工程と、

前記復号化により再現された元のデジタルデータを再生出力する再生工程と、

を含むことを特徴とするデジタルデータ再生方法。

【請求項13】 前記演算工程は、前記暗号化デジタルデータの任意の場所に埋め込まれた特定のデータ改ざ

ん検出コードの検出の有無に基づき、デジタルデータの改ざんの有無を判断し、不正改ざんと判断した場合には、再生しないことを特徴とする請求項12に記載のデジタルデータ再生方法。

【請求項14】 前記請求項8～13のいずれか一つに記載された方法をコンピュータに実行させることを特徴とするプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、デジタルデータを暗号処理するデジタルデータ暗号システムと、暗号処理されたデジタルデータを再生する音楽プレイヤー、音楽再生機能を有したデジタルカメラなどを含むデジタルデータ暗号システム、デジタルデータ再生装置、デジタルデータ暗号方法およびその方法をコンピュータに実行させるプログラムに関する。

【0002】

【従来の技術】近年、音楽データなどのデジタルデータの高圧縮技術、たとえば、MP3(MPEG3)などにより、フラッシュメモリを用いた携帯音楽プレイヤーなどのデジタルデータ再生装置が開発、発売されている。デジタルデータ再生装置のフラッシュメモリに格納されたデジタルデータは、高圧縮技術によりデータ容量が少なく、少ないメモリ容量で長時間の音楽データを再生できるため、携帯性に優れる、消費電力が少なく、軽量化が図れるなどの利点を有している。

【0003】

【発明が解決しようとする課題】このような、デジタルデータ再生装置で再生されるデジタルデータ、たとえば、音楽データは著作物であるが、高圧縮されていることにより、データ容量が少ないため短時間に転送でき、またフラッシュメモリなどの小型な記録媒体に格納して容易に携帯可能なため、不正な配布および利用がなされるという問題が生じている。

【0004】上記問題に対応するため、現在、著作物であるデジタルデータの不正な配布、使用を防止するための各種手段が提案されている。たとえば、フラッシュメモリカードを使用した携帯音楽プレイヤーは、あらかじめ著作権保護機能を有したフラッシュメモリカードを使用する構成であり、フラッシュメモリカードと、音楽プレイヤーとの間で、認証システムを使用して著作権を保護しようとするものであるが、このような方式では、ユーザーが使用するパーソナルコンピュータのオペレーティングシステム(OS)の利用条件などに大きな制約を生じる問題がある。

【0005】また、フラッシュメモリカードを用いて再生する携帯音楽プレイヤーなどのデジタルデータ再生装置に著作権保護の方式を適用したもので、この携帯音楽プレイヤーの電気回路の実装構成が変更となり、それにもなって開発コストが増加する問題がある。

【0006】この発明は、上述した従来技術による問題を解消するため、デジタルデータの著作権を保護することができ、この保護をパーソナルコンピュータなどの使用条件に制約をおよぼすことなく、また、デジタルデータ再生装置のコストに影響を与えずに実現できるデジタルデータ暗号システムおよびデジタルデータ再生装置の提供を目的とする。

【0007】

【課題を解決するための手段】上述した課題を解決し、目的を達成するため、請求項1に記載の発明にかかるデジタルデータ暗号システムは、入力されたデジタルデータを所定の暗号アルゴリズムおよび暗号演算式作成パラメータに基づき決定される暗号演算式にしたがって、暗号処理をおこなう演算手段と、前記暗号化されたデジタルデータとともに、暗号処理に用いた暗号アルゴリズムを一意に決定可能なインデックス値と暗号演算式作成パラメータを、同一のファイルに作成出力するファイル手段と、を備えたことを特徴とする。

【0008】この請求項1の発明によれば、著作物などのデジタルデータを、暗号化することによって、不正な配布を防止してデジタルデータの著作権を保護できるようになる。また、暗号化に使用する暗号アルゴリズムと、暗号演算式作成パラメータを同一のファイル内に記述するため、復号を容易におこなえるようになる。

【0009】また、請求項2の発明にかかるデジタルデータ暗号システムは、請求項1に記載の発明において、実際の暗号化に使用する暗号アルゴリズムがあらかじめ複数設定登録された設定手段を備え、前記暗号処理時に所定の暗号アルゴリズムが選択可能なことを特徴とする。

【0010】この請求項2の発明によれば、複数の暗号アルゴリズムから、実際に暗号化に使用する暗号アルゴリズムを複数の中から選択可能であるため、暗号化のルールを複雑化でき、暗号化デジタルデータの解読の可能性を低減化できるようになる。

【0011】また、請求項3の発明にかかるデジタルデータ暗号システムは、請求項1に記載の発明において、前記演算手段は、前記暗号処理時に、あらかじめ用意された複数の暗号アルゴリズムおよび暗号演算式作成パラメータの中から実際の暗号化に使用する暗号アルゴリズムおよび暗号演算式作成パラメータを選択し、該選択した暗号アルゴリズムおよび暗号演算式作成パラメータを用いて、暗号処理をおこなうことを特徴とする。

【0012】この請求項3の発明によれば、複数の暗号アルゴリズムから、実際に暗号化に使用する暗号アルゴリズムを複数から選択可能であり、複数デジタルデータの暗号化をおこなう場合に、暗号アルゴリズムと暗号演算式作成パラメータを変化させることによって、暗号化のルールをより複雑化でき、暗号化デジタルデータの解読の可能性をより低減化できるようになる。

【0013】また、請求項4の発明にかかるデジタルデータ暗号システムは、請求項1～3のいずれか一つに記載の発明において、前記演算手段は、前記暗号アルゴリズムに基づきデジタルデータの任意の場所に特定のデータ改ざん検出コードを埋め込み暗号処理を実行することにより、デジタルデータの不正改ざんを検出可能なことを特徴とする。

【0014】この請求項4の発明によれば、データ改ざん検出コードに基づき暗号化されたデジタルデータに対する改ざんの有無を検出でき、デジタルデータが正規のものであるか不正改ざんされたものであるかを判断できるようになる。

【0015】また、請求項5の発明にかかるデジタルデータ暗号システムは、請求項1～4のいずれか一つに記載の発明において、前記ファイル手段は、前記暗号化デジタルデータと同一ファイルに格納する暗号アルゴリズムのインデックス値および暗号演算式作成パラメータの記載箇所を容易に特定できない状態となるようデータ変更を施すことを特徴とする。

【0016】この請求項5の発明によれば、暗号デジタルデータと同一ファイル内に記述された、暗号アルゴリズムのインデックス値および暗号演算パラメータを隠匿することができるので、暗号演算式が不正に解釈されることを防止できるようになる。

【0017】また、請求項6の発明にかかるデジタルデータ再生装置は、請求項1～5のいずれか一つに記載のデジタルデータ暗号システムにより生成された暗号化デジタルデータから著作物デジタルデータを復号、再生するデジタルデータ再生装置であって、前記暗号化されたデジタルデータを取り込む読み取り手段と、前記暗号化されたデジタルデータと同一ファイル内に記載された暗号アルゴリズムのインデックス値、および暗号演算式作成パラメータに基づく暗号演算式を決定し、その演算式にしたがって前記暗号化されたデジタルデータの復号処理をおこなう演算手段と、前記復号化により再現された元のデジタルデータを再生出力する再生手段と、を備えたことを特徴とする。

【0018】この請求項6の発明によれば、再生装置で再生することを目的に作成され暗号化されたデジタルデータは、同一ファイル内の暗号アルゴリズムのインデックス値、および暗号演算式作成パラメータに基づく暗号演算式を用いて復号処理されるので、暗号処理と対になる復号処理によってのみデジタルデータを再生することができるようになり、作成したデータを不正に配布した場合にはこの再生装置やパーソナルコンピュータなどでの再生を不可にでき、デジタルデータの著作権を保護できるようになる。

【0019】また、請求項7の発明にかかるデジタルデータ再生装置は、請求項6に記載の発明において、前記演算手段は、前記暗号化デジタルデータの任意の場

所に埋め込まれた特定のデータ改ざん検出コードの検出の有無に基づき、デジタルデータの改ざんの有無を判断し、不正改ざんと判断した場合には、再生しないことを特徴とする。

【0020】この請求項7の発明によれば、暗号化されたデジタルデータに埋め込まれたデータ改ざん検出コードの検出の有無でデジタルデータの不正改ざんを検出することができ、この場合デジタルデータの再生をおこなわないため不正な復号による再生を不可能にでき、デジタルデータの著作権を保護できるようになる。

【0021】また、請求項8の発明にかかるデジタルデータ暗号方法は、入力されたデジタルデータを所定の暗号アルゴリズムおよび暗号演算式作成パラメータに基づき決定される暗号演算式にしたがって、暗号処理をおこなう演算工程と、前記暗号化されたデジタルデータとともに、暗号処理に用いた暗号アルゴリズムを一意に決定可能なインデックス値と暗号演算式作成パラメータを、同一のファイルに作成出力するファイル工程と、を含んだことを特徴とする。

【0022】この請求項8の発明によれば、著作物などのデジタルデータを、簡単な手順で暗号化でき、不正な配布を防止してデジタルデータの著作権を保護できるようになる。また、暗号化に使用する暗号アルゴリズムと、暗号演算式作成パラメータを同一のファイル内に記述するため、復号を容易におこなえるようになる。

【0023】また、請求項9の発明にかかるデジタルデータ暗号方法は、請求項8に記載の発明において、前記演算工程は、あらかじめ用意された複数の暗号アルゴリズムおよび暗号演算式作成パラメータの中から実際の暗号化に使用する暗号アルゴリズムおよび暗号演算式作成パラメータを選択し、該選択した暗号アルゴリズムおよび暗号演算式作成パラメータを用いて、暗号処理をおこなうことを特徴とする。

【0024】この請求項9の発明によれば、複数の暗号アルゴリズムから、実際に暗号化に使用する暗号アルゴリズムを複数から選択可能であり、複数デジタルデータの暗号化をおこなう場合に、暗号アルゴリズムと暗号演算式作成パラメータを変化させることによって、暗号化のルールをより複雑化でき、暗号化デジタルデータの解読の可能性をより低減化できるようになる。

【0025】また、請求項10の発明にかかるデジタルデータ暗号方法は、請求項8、9のいずれか一つに記載の発明において、前記演算工程は、前記暗号アルゴリズムに基づきデジタルデータの任意の場所に特定のデータ改ざん検出コードを埋め込み暗号処理を実行することにより、デジタルデータの不正改ざんを検出可能なことを特徴とする。

【0026】この請求項10の発明によれば、データ改ざん検出コードに基づき暗号化されたデジタルデータ

に対する改ざんの有無が検出でき、デジタルデータが正規のものであるか不正改ざんされたものであるかを判断できるようになる。

【0027】また、請求項11の発明にかかるデジタルデータ暗号方法は、請求項8～10のいずれか一つに記載の発明において、前記演算工程は、前記暗号化デジタルデータと同一ファイルに格納する暗号アルゴリズムのインデックス値および暗号演算式作成パラメータの記載箇所を容易に特定できない状態となるようデータ変更を施すことを特徴とする。

【0028】この請求項11の発明によれば、暗号デジタルデータと同一ファイル内に記述された、暗号アルゴリズムのインデックス値および暗号演算パラメータを隠匿することができるので、暗号演算式が不正に解釈されることを防止できるようになる。

【0029】また、請求項12の発明にかかるデジタルデータ再生方法は、請求項8～10のいずれかのデジタルデータ暗号方法により生成された暗号化デジタルデータから著作物デジタルデータを復号、再生するデジタルデータ再生方法であって、前記暗号化されたデジタルデータを取り込む読み取り工程と、前記暗号化されたデジタルデータと同一ファイル内に記載された暗号アルゴリズムのインデックス値、および暗号演算式作成パラメータに基づく暗号演算式を決定し、その演算式にしたがって前記暗号化されたデジタルデータの復号処理をおこなう演算工程と、前記復号化により再現された元のデジタルデータを再生出力する再生工程と、を含むことを特徴とする。

【0030】この請求項12の発明によれば、再生装置で再生することを目的に作成され暗号化されたデジタルデータは、同一ファイル内の暗号アルゴリズムのインデックス値、および暗号演算式作成パラメータに基づく暗号演算式を用いて復号処理されるので、暗号処理と対になる復号処理によってのみデジタルデータを再生することができるようになり、作成したデータを不正に配布した場合にはこの再生装置やパーソナルコンピュータなどでの再生を不可にでき、デジタルデータの著作権を保護できるようになる。

【0031】また、請求項13の発明にかかるデジタルデータ再生方法は、請求項12に記載の発明において、前記演算工程は、前記暗号化デジタルデータの任意の場所に埋め込まれた特定のデータ改ざん検出コードの検出の有無に基づき、デジタルデータの改ざんの有無を判断し、不正改ざんと判断した場合には、再生しないことを特徴とする。

【0032】この請求項13の発明によれば、暗号化されたデジタルデータに埋め込まれたデータ改ざん検出コードの検出の有無でデジタルデータの不正改ざんを検出することができ、この場合デジタルデータの再生をおこなわないため不正な復号による再生を不可能に

き、デジタルデータの著作権を保護できるようになる。

【0033】また、請求項14の発明にかかるプログラムは、請求項8～13のいずれか一つに記載された方法をコンピュータに実行させることを特徴とする。

【0034】この請求項14の発明によれば、請求項8～13に記載された方法をコンピュータに実行させることができ、コンピュータを用いてデジタルデータの暗号処理、および復号再生処理を実行できるようになる。

10 【0035】

【発明の実施の形態】以下に添付図面を参照して、この発明にかかるデジタルデータ暗号システム、デジタルデータ再生装置、デジタルデータ暗号方法およびその方法をコンピュータに実行させるプログラムの好適な実施の形態を詳細に説明する。

【0036】（実施の形態1）図1は、本発明のデジタルデータ暗号システムの要部である暗号データ生成部の構成を示すブロック図である。図1において、暗号データ生成部101は、著作物デジタルデータが入力される入力手段102と、CPUなどからなり、入力手段102に入力された著作物デジタルデータに対する暗号化処理をおこなう演算手段103と、ハードディスク、フラッシュメモリなどからなり、演算手段103で暗号化された暗号化デジタルデータをファイル化して出力するファイル手段104と、演算手段103による暗号化処理のための暗号アルゴリズム、暗号演算式作成パラメータが登録設定されている設定手段105によって構成される。

【0037】入力手段102は、ハードディスクやCD-ROMなどの記録媒体のデータを読み出すドライブ装置を用いて構成できる。ファイル手段104は、ハードディスクやフラッシュメモリなどの記録媒体にデータを書き込むドライブ装置を用いて構成できる。設定手段105は、ROM、RAMなどの記憶装置を用いて構成することができる。以上の構成からなる暗号データ生成部101は、汎用のパーソナルコンピュータを用い、演算手段103を以下に説明する手順で暗号化処理するプログラムを実行制御して構成できる。

【0038】つぎに、上述した暗号データ生成部による著作物デジタルデータの暗号化手順を、図2のフローチャートにしたがって説明する。演算手段103は、入力手段102を介し入力された著作物デジタルデータを読み出す（ステップS201）。つぎに、実際の暗号化に使用する暗号アルゴリズム（暗号演算式）を決定（選択）する（ステップS202）。

【0039】設定手段105には、あらかじめ複数の暗号アルゴリズムが登録設定されており、演算手段103は、一つの暗号アルゴリズムを選択する。具体的には、この暗号アルゴリズムの選択は、ユーザーの操作選択により、あるいは演算手段103により自動選択される。

【0040】つぎに、演算手段103は、選択された暗号アルゴリズムに用いる暗号演算式作成パラメータの決定をおこなう（ステップS203）。この暗号演算式作成パラメータは、演算手段103によって自動的に設定される。上記の暗号アルゴリズムと、暗号演算式作成パラメータの設定により、実際に暗号処理をおこなう暗号演算式 $f(x)$ が決定されることになる。暗号演算式 $f(x)$ の決定方法は、上記選択した暗号アルゴリズム内に含まれる。

【0041】つぎに、演算手段103により、上記暗号演算式 $f(x)$ を用いて著作物デジタルデータに対する暗号化演算を実行する（ステップS204）。以下に、暗号化の具体例を説明する。まず、暗号化対象となる著作物デジタルデータを、ある整数の集合 $(X1, X2, X3 \dots)$ とみなす。どのような形の整数とするかについては、暗号アルゴリズムが示す手順を適用する。たとえば、暗号対象の著作物デジタルデータを整数の集合とし、暗号演算式 $f(x)$ にしたがって、それらの整数に下記演算を施す。

【0042】 $Y1 = f(X1)$,
 $Y2 = f(X2)$,
 $Y3 = f(X3)$,
 \dots
 $Yn = f(Xn)$

【0043】そして、上記演算後の整数の集合 $(Y1, Y2, Y3, \dots, Yn)$ を作成し、演算後の整数の集合を暗号化デジタルデータとして生成する。

【0044】つぎに、ファイル手段104は、暗号データ作成に使用した暗号アルゴリズムのインデックス値、および、暗号演算式作成パラメータを、演算後の暗号化デジタルデータ $(Y1, Y2, Y3, \dots, Yn)$ とともに同一ファイル化する（ステップS205）。ファイル化された暗号化デジタルデータは、フラッシュメモリなどの記憶媒体に書込保存される。

【0045】この暗号化デジタルデータの再生は、後述するが、ファイル内の所定の箇所に記載されている暗号アルゴリズムのインデックス値を読み込み、この暗号アルゴリズムのインデックス値から決定される暗号演算式作成パラメータの記述箇所を参照することで、復号に必要な情報を取得して復号演算式を作成し、その復号演算式に基づいて復号処理をおこない、再生できるようにする。

【0046】上記の暗号化演算により作成された暗号化デジタルデータは、本来の著作物デジタルデータから一般的には意味をなさない形式のデータに変換される。このため、この暗号化デジタルデータは、上述した暗号データ生成部101と対をなす特定の復号処理をおこなう復号装置を用いない限り、再生することができないこととなる。このような暗号化デジタルデータは、汎用的な環境では再生、および使用できないデータ

であるため、不正に配布されたとしても、その不正利用を防止することができる。

【0047】特に、暗号化時には、複数の暗号アルゴリズムから、実際に暗号化に使用する暗号アルゴリズム、暗号演算式作成パラメータの組み合わせを複数の中から選択するため、暗号化のルールを複雑化でき、暗号化デジタルデータの解読の可能性を低減化できるようになる。

【0048】演算手段103は、暗号化前の著作物デジタルデータと、暗号化後の暗号化デジタルデータを読み出した元の記憶媒体（入力手段102あるいはファイル手段104）に対し出力し書き込む構成としてもよい。

【0049】（実施の形態2）図3は、本発明の実施の形態2による著作物デジタルデータの暗号化手順を示すフローチャートである。同図において、実施の形態1（図2記載）で説明した各処理と同一の処理内容には同一の符号を附して説明を省略する。

【0050】この実施の形態2では、演算手段103は、上記の暗号化演算（ステップS204）の実行前に、改ざん防止データ（データ改ざん検出コード）の埋め込み処理を実行する（ステップS301）。具体的には、暗号対象となる著作物デジタルデータの任意の場所に、特定のデータ改ざん検出コードを埋め込むものとする。このデータ改ざん検出コードを埋め込む場所、コードの個数、コードの内容に関しては、ステップS202で選択された暗号アルゴリズムによって決定される。

【0051】そして、このデータ改ざん検出コードを埋め込んだ著作物デジタルデータに対してステップS204で暗号演算する。これにより、暗号処理後における暗号化デジタルデータに対するデータ改ざんの有無は、この暗号化デジタルデータを復号し、その中のデータ改ざん検出コードを検出し、このデータ改ざん検出コードが特定の埋め込み場所、コードの個数、コードの内容に完全一致すればデータ改ざんがないと判断でき、いずれかでも不一致時にはデータが改ざんされていると判断できるようになる。

【0052】上記実施の形態で説明したデジタルデータ暗号システムでは、暗号化デジタルデータとともに、暗号演算式を決定する情報（暗号アルゴリズムのインデックス値と、暗号演算式作成パラメータ）が一つのファイルとして作成される構成とした。この暗号演算式を決定する情報（暗号アルゴリズムのインデックス値と、暗号演算式作成パラメータ）が、外部からファイル中の記載箇所（たとえばエリア）を容易に特定できない状態となるよう所定のデータ変更を施す処理をおこなう構成としてもよい。

【0053】たとえば、実際の暗号演算式を決定する情報とともに、暗号演算式を決定する情報以外の不必要な情報（たとえば乱数などの無意味なデータ列）を同一フ

ファイル中に記載する。この場合、暗号演算式を決定する情報には、不必要な情報を示すデータ（たとえば上記不必要な情報の記載エリア）を付帯させる。なお、暗号化デジタルデータの復号化処理時には、暗号演算式を決定する情報に基づき、暗号演算式を決定する情報以外の不必要な情報を削除処理する。

【0054】（実施の形態3）つぎに、本発明のデジタルデータ再生装置の実施形態について説明する。このデジタルデータ再生装置は、上記の実施形態で説明した暗号化デジタルデータを復号化して著作物デジタルデータを再生する装置である。この暗号化デジタルデータは、上述した暗号データ生成部101のファイル手段104によりファイル化し書き込んだ挿抜可能なフラッシュメモリなどの記録媒体にデータ記録されており、この記録媒体を再生装置の読み出し装置に装着して再生処理をおこなうことができる。

【0055】図4は、本発明のデジタルデータ再生装置の構成を示すブロック図である。デジタルデータ再生装置401は、上記の暗号化デジタルデータが記録された記録媒体を読み取る読み取り手段402と、CPUなどからなり、読み取り手段402により記録媒体から読み出した暗号化デジタルデータから元の著作物デジタルデータを復号化処理する演算手段403と、演算手段403による復号により得られる元の著作物デジタルデータを再生する再生手段404によって構成される。

【0056】図5は、本発明のデジタルデータ再生装置によるデジタルデータ再生時のフローチャートである。デジタルデータ再生装置401の読み取り手段402は、記録媒体に記録されたファイルを読み出す（ステップS501）。つぎに、ファイル内の所定の箇所に記載されている暗号アルゴリズムのインデックス値を読み込む（ステップS502）。つぎに、読み出した暗号アルゴリズムのインデックス値から決定される、暗号演算式作成パラメータの記述されている箇所を参照して暗号演算式作成パラメータを得る（ステップS503）。これにより、暗号化デジタルデータの復号化処理に必要な情報を取得できる。

【0057】つぎに、これら取得した情報（暗号アルゴリズムのインデックス値、暗号演算式作成パラメータ）に基づき復号演算式を作成する（ステップS504）。この後、これら取得した情報と同一ファイルに格納されている暗号化デジタルデータを復号演算式に基づいて復号処理をおこなう（ステップS505）。これにより、暗号処理される前の著作物デジタルデータを復元することができ、再生手段404により、著作物デジタルデータの形式に対応した再生がおこなえるようになる（ステップS506）。

【0058】（実施の形態4）図6は、本発明の実施の形態4による暗号化デジタルデータの復号化手順を示

すフローチャートである。同図において、実施の形態3（図5記載）で説明した各処理と同一の処理内容には同一の符号を附して説明を省略する。

【0059】この実施の形態4では、演算手段403は、上記の復号処理中に、データ改ざんの有無を判断する手順を追加したものである。暗号化デジタルデータには、任意の場所に、特定のデータ改ざん検出コードが埋め込まれており、ステップS505の復号処理後に、このデータ改ざん検出コードが検出されれば（ステップS601：Yes）、データ改ざんがなくデータ再生が可能と判断して再生を続ける（ステップS602）。一方、データ改ざん検出コードが検出されない場合には（ステップS601：No）、データ改ざんの可能性があり、少なくともデータ再生エラーと判断して再生を中止させる（ステップS603）。

【0060】データ改ざん検出コードの検出の具体例は、たとえば、特定の埋め込み場所、コードの個数、コードの内容に完全一致すればデータ改ざんがないと判断し、いずれかでも不一致時にはデータが改ざんされていると判断する。

【0061】図6のフローチャートにおける復号化対象の著作物デジタルデータは、音楽データなど所定の再生時間を有するデジタルデータの例を示すものである。このようなデータ形式の場合には、暗号化デジタルデータ全ての再生が終了するまでの期間中は（ステップS604：No）、上記ステップS505における復号処理と、データ改ざんの検出処理を順次おこないながら、ステップS501に復帰して暗号化デジタルデータを継続的に読み込み処理することになる。そして、暗号化デジタルデータ全ての再生の終了（ステップS604：Yes）に基づき再生にかかる処理を終了する。

【0062】本発明では、音楽配信などに特化した高度な著作権保護方式ではなく、デジタルデータ再生装置用に作成された著作物デジタルデータが不正に配布された場合に再生不能とするよう暗号処理することにより、著作物デジタルデータを保護する構成のものであり、特にユーザーの使用環境や、開発コストに影響をおよぼさずに実現できるようにしたものである。

【0063】そして、本発明のデジタルデータ暗号化システムの各構成は、著作権デジタルデータの暗号化処理時に任意の暗号演算式を用いて暗号化デジタルデータを作成し、暗号化デジタルデータを格納する同一ファイルに暗号化演算に用いた暗号アルゴリズムのインデックス値、および暗号演算式作成パラメータをともに格納する構成であるため、汎用のコンピュータ装置を用いて著作権デジタルデータの暗号化をOSなどに制約を与えず容易におこなえるものである。

【0064】また、上記説明した本発明のデジタルデータ再生装置の各構成は、フラッシュメモリなどの半導体メモリを使用した音楽プレイヤーや、音楽再生機能を

有したデジタルカメラなどのデジタルデータ再生装置に適用することができ、これら再生装置において再生するデジタルデータの著作権を保護できるようになる。また、デジタルデータ再生装置側では、暗号化デジタルデータに含まれる暗号アルゴリズムのインデックス値、および暗号演算式作成パラメータに基づき復号化演算を実行できるので、復号化のための特別な構成が不要で装置コストを抑えてデジタルデータの著作権保護を実現できるようになる。

【0065】上記各実施の形態では、暗号化デジタルデータをフラッシュメモリなどの記録媒体に格納し、これを再生する構成を例に説明したが、これに限らず、コンピュータ装置にて生成された暗号化デジタルデータをデジタルデータ再生装置に転送する構成としては、これらコンピュータ装置とデジタルデータ再生装置との間を所定のデータ伝送形式でコネクタおよびケーブルを用いた接続で伝送する構成や、インターネットなどのネットワークを介して伝送する構成とすることができ、この場合においても上記同様の作用効果を得ることができる。

【0066】なお、本実施の形態で説明したデジタルデータの暗号化方法は、あらかじめ用意された暗号化のプログラムを汎用のコンピュータ装置で実行することにより実現することができる。このプログラムは、ハードディスク、フロッピー（登録商標）ディスク、CD-ROM、MO、DVDなどのコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行される。またこのプログラムは、上記記録媒体を介して、インターネットなどのネットワークを介して配布することができる。また、暗号化デジタルデータの復号化についても、デジタルデータ再生装置に適用するのみならず、復号化のプログラムを汎用のコンピュータ装置で実行することにより実現することができる。

【0067】

【発明の効果】以上説明したように、請求項1に記載の発明によれば、入力されたデジタルデータを所定の暗号アルゴリズムおよび暗号演算式作成パラメータに基づき決定される暗号演算式にしたがって、暗号処理をおこなう演算手段と、前記暗号化されたデジタルデータとともに、暗号処理に用いた暗号アルゴリズムを一意に決定可能なインデックス値と暗号演算式作成パラメータを、同一のファイルに作成出力するファイル手段とを備えたので、著作物などのデジタルデータの暗号化によって、不正な配布を防止してデジタルデータの著作権を保護できるようになる。また、暗号化に使用する暗号アルゴリズムと、暗号演算式作成パラメータを同一のファイル内に記述するため、復号を容易におこなう復号にかかる構成を簡単に構成できる。この著作権保護は、パーソナルコンピュータなどの使用条件に制約をおよぼす

ことなく実現できるという効果を奏する。

【0068】また、請求項2に記載の発明によれば、請求項1に記載の発明において、実際の暗号化に使用する暗号アルゴリズムがあらかじめ複数設定登録された設定手段を備え、前記暗号処理時に所定の暗号アルゴリズムが選択可能としたので、複数の暗号アルゴリズムから、実際に暗号化に使用する暗号アルゴリズムを複数の中から選択可能であるため、暗号化のルールを複雑化でき、暗号化デジタルデータの解読の可能性を低減化できるという効果を奏する。

【0069】また、請求項3に記載の発明によれば、請求項1に記載の発明において、前記演算手段は、前記暗号処理時に、あらかじめ用意された複数の暗号アルゴリズムおよび暗号演算式作成パラメータの中から実際の暗号化に使用する暗号アルゴリズムおよび暗号演算式作成パラメータを選択し、該選択した暗号アルゴリズムおよび暗号演算式作成パラメータを用いて、暗号処理をおこなうので、複数の暗号アルゴリズムから、実際に暗号化に使用する暗号アルゴリズムを複数から選択可能であり、複数デジタルデータの暗号化をおこなう場合に、暗号アルゴリズムと暗号演算式作成パラメータを変化させることによって、暗号化のルールをより複雑化でき、暗号化デジタルデータの解読の可能性をより低減化できるという効果を奏する。

【0070】また、請求項4に記載の発明によれば、請求項1～3のいずれか一つに記載の発明において、前記演算手段は、前記暗号アルゴリズムに基づきデジタルデータの任意の場所に特定のデータ改ざん検出コードを埋め込み暗号処理を実行するので、暗号化されたデジタルデータに対する改ざんの有無を検出でき、デジタルデータが正規のものであるか不正改ざんされたものであるかを判断できるという効果を奏する。

【0071】また、請求項5に記載の発明によれば、請求項1～4のいずれか一つに記載の発明において、前記演算手段は、前記暗号化デジタルデータと同一ファイルに格納する暗号アルゴリズムのインデックス値および暗号演算式作成パラメータの記載箇所を容易に特定できない状態となるようデータ変更を施すので、暗号デジタルデータと同一ファイル内に記述された、暗号アルゴリズムのインデックス値および暗号演算パラメータを隠匿することができ、暗号演算式が不正に解読されることを防止できるという効果を奏する。

【0072】また、請求項6に記載の発明によれば、請求項1～5のいずれか一つに記載のデジタルデータ暗号システムにより生成された暗号化デジタルデータから著作物デジタルデータを復号、再生するデジタルデータ再生装置であって、前記暗号化されたデジタルデータを取り込む読み取り手段と、前記暗号化されたデジタルデータと同一ファイル内に記載された暗号アルゴリズムのインデックス値、および暗号演算式作成パラ

メータに基づく暗号演算式を決定し、その演算式にしたがって前記暗号化されたデジタルデータの復号処理をおこなう演算手段と、前記復号化により再現された元のデジタルデータを再生出力する再生手段と、を備えたので、再生装置で再生することを目的に作成され暗号化されたデジタルデータは、同一ファイル内の暗号アルゴリズムのインデックス値、および暗号演算式作成パラメータに基づく暗号演算式を用いて復号処理され、暗号処理と対になる復号処理によってのみデジタルデータを再生することができるようになり、作成したデータを不正に配布した場合にはこの再生装置やパーソナルコンピュータなどでの再生を不可にでき、デジタルデータの著作権を保護できる。この著作権保護は、デジタルデータ再生装置のコストに影響を与えずに実現できるという効果を奏する。

【0073】また、請求項7に記載の発明によれば、請求項6に記載の発明において、前記演算手段は、前記暗号化デジタルデータの任意の場所に埋め込まれた特定のデータ改ざん検出コードの検出の有無に基づき、デジタルデータの改ざんの有無を判断し、不正改ざんと判断した場合には、再生しないので、暗号化されたデジタルデータに埋め込まれたデータ改ざん検出コードの検出の有無でデジタルデータの不正改ざんを検出することができ、この場合デジタルデータの再生をおこなわないため不正な復号による再生を不可能にでき、デジタルデータの著作権を保護できるという効果を奏する。

【0074】また、請求項8に記載の発明によれば、入力されたデジタルデータを所定の暗号アルゴリズムおよび暗号演算式作成パラメータに基づき決定される暗号演算式にしたがって、暗号処理をおこなう演算工程と、前記暗号化されたデジタルデータとともに、暗号処理に用いた暗号アルゴリズムを一意に決定可能なインデックス値と暗号演算式作成パラメータを、同一のファイルに作成出力するファイル工程と、を含んだので、著作物などのデジタルデータを、簡単な手順で暗号化でき、不正な配布を防止してデジタルデータの著作権を保護できるようになる。また、暗号化に使用する暗号アルゴリズムと、暗号演算式作成パラメータを同一のファイル内に記述するため、復号を容易におこなえるという効果を奏する。

【0075】また、請求項9に記載の発明によれば、請求項8に記載の発明において、前記演算工程は、あらかじめ用意された複数の暗号アルゴリズムおよび暗号演算式作成パラメータの中から実際の暗号化に使用する暗号アルゴリズムおよび暗号演算式作成パラメータを選択し、該選択した暗号アルゴリズムおよび暗号演算式作成パラメータを用いて、暗号処理をおこなうので、複数の暗号アルゴリズムから、実際に暗号化に使用する暗号アルゴリズムを複数から選択可能であり、複数デジタルデータの暗号化をおこなう場合に、暗号アルゴリズムと

暗号演算式作成パラメータを変化させることによって、暗号化のルールをより複雑化でき、暗号化デジタルデータの解読の可能性をより低減化できるという効果を奏する。

【0076】また、請求項10に記載の発明によれば、請求項8、9のいずれか一つに記載の発明において、前記演算工程は、前記暗号アルゴリズムに基づきデジタルデータの任意の場所に特定のデータ改ざん検出コードを埋め込み暗号処理を実行するので、データ改ざん検出コードに基づき暗号化されたデジタルデータに対する改ざんの有無が検出でき、デジタルデータが正規のものであるか不正改ざんされたものであるかを判断できるという効果を奏する。

【0077】また、請求項11に記載の発明によれば、請求項8～10のいずれか一つに記載の発明において、前記演算工程は、前記暗号化デジタルデータと同一ファイルに格納する暗号アルゴリズムのインデックス値および暗号演算式作成パラメータの記載箇所を容易に特定できない状態となるようデータ変更を施すので、暗号化デジタルデータと同一ファイル内に記述された、暗号アルゴリズムのインデックス値および暗号演算パラメータを隠匿することができ、暗号演算式が不正に解読されることを防止できるという効果を奏する。

【0078】また、請求項12に記載の発明によれば、請求項8～10のいずれかのデジタルデータ暗号方法により生成された暗号化デジタルデータから著作物デジタルデータを復号、再生するデジタルデータ再生方法であって、前記暗号化されたデジタルデータを取り込む読み取り工程と、前記暗号化されたデジタルデータと同一ファイル内に記載された暗号アルゴリズムのインデックス値、および暗号演算式作成パラメータに基づく暗号演算式を決定し、その演算式にしたがって前記暗号化されたデジタルデータの復号処理をおこなう演算工程と、前記復号化により再現された元のデジタルデータを再生出力する再生工程と、を含むので、再生装置で再生することを目的に作成され暗号化されたデジタルデータは、同一ファイル内の暗号アルゴリズムのインデックス値、および暗号演算式作成パラメータに基づく暗号演算式を用いて復号処理され、暗号処理と対になる復号処理によってのみデジタルデータを再生することができるようになり、作成したデータを不正に配布した場合にはこの再生装置やパーソナルコンピュータなどでの再生を不可にでき、デジタルデータの著作権を保護できるという効果を奏する。

【0079】また、請求項13に記載の発明によれば、請求項12に記載の発明において、前記演算工程は、前記暗号化デジタルデータの任意の場所に埋め込まれた特定のデータ改ざん検出コードの検出の有無に基づき、デジタルデータの改ざんの有無を判断し、不正改ざんと判断した場合には、再生しないので、暗号化されたデ

デジタルデータに埋め込まれたデータ改ざん検出コードの検出の有無でデジタルデータの不正改ざんを検出することができ、この場合デジタルデータの再生をおこなわないため不正な復号による再生を不可能にでき、デジタルデータの著作権を保護できるという効果を奏する。

【0080】また、請求項14に記載の発明によれば、請求項8～13のいずれか一つに記載された方法をコンピュータに実行させるので、コンピュータを用いてデジタルデータの暗号処理、および復号再生処理を実行できるという効果を奏する。

【図面の簡単な説明】

【図1】この発明の本実施の形態にかかるデジタルデータ暗号システムの構成を示すブロック図である。

【図2】この発明の本実施の形態にかかるデジタルデータ暗号システムによる暗号処理を示すフローチャートである。

【図3】この発明の本実施の形態にかかるデジタルデータ暗号システムによる他の暗号処理を示すフローチャートである。

ートである。

【図4】この発明の本実施の形態にかかるデジタルデータ再生装置の構成を示すブロック図である。

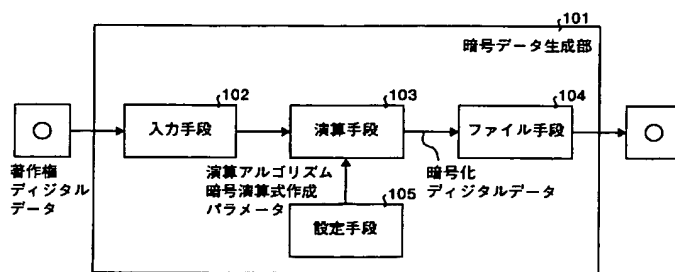
【図5】この発明の本実施の形態にかかるデジタルデータ再生装置による復号処理を示すフローチャートである。

【図6】この発明の本実施の形態にかかるデジタルデータ再生装置による復号処理を示すフローチャートである。

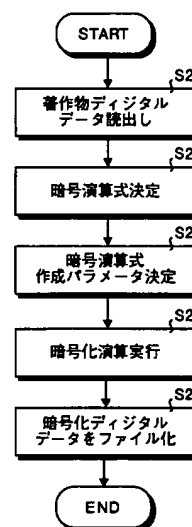
【符号の説明】

- 101 暗号データ生成部
- 102 入力手段
- 103 演算手段
- 104 ファイル手段
- 105 設定手段
- 401 デジタルデータ再生装置
- 402 読み取り手段
- 403 演算手段
- 404 再生手段

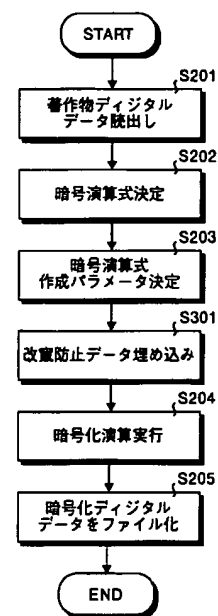
【図1】



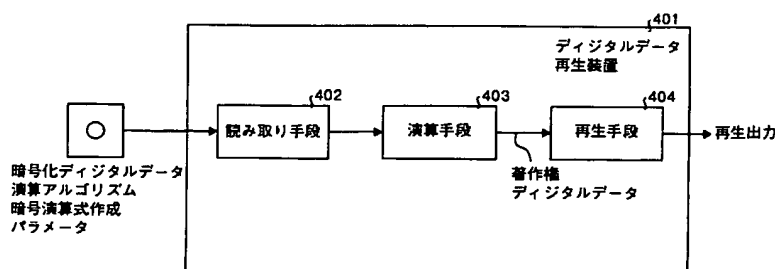
【図2】



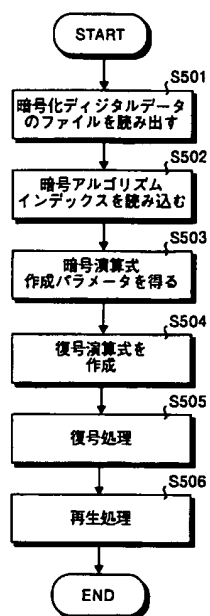
【図3】



【図4】



【図5】



【図6】

